DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 8/23/2011 has been entered.

Response to Arguments

2. 1. This action is responsive to communications filed 8/23/2011. Claims 1-21, 33 and 34 are pending in the case. Claims 22 to 32 are cancelled by the applicant.

Applicant's argument is based on the new features added via amendment, and hence is moot in view of the new grounds of rejection outlined in the following.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-21 and 33 and 34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. All claims include a security policy including an abstract cryptographic object. However, the only place that abstract cryptographic objects are mentioned in the spec is in paragraph [0051] (published application). It mentions a distributed security system that may abstract cryptographic objects and operations to make the system independent of the underlying cryptographic technology. However, no teaching of a security policy including such object, or its description is found.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 34 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Said claim is directed to a Computer Readable Medium (CRM). The instructions on the CRM are not necessarily executed. CRM are generally considered to include signals, which are non-statutory.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 3, and 5 to 19, 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel (U.S. Patent No. 6678827) in view of Gensler, JR, et al. (U.S. Patent Application Publication No. 2003/0046574), hereinafter called Gen.

6.1. As per claim 1, Rothermel is directed to a distributed security system (Fig. 1 and column 4 line 63 to column 5 line 13) comprising:

a security policy written in a security protocol independent (column 7 line 3 to 57 disclose that the Security Policy Manager Device allows a user to create a security template independent of security protocols running in NSDs. The template will be configured based on NSD protocols to create a security policy compatible with NSD, once the template is loaded on NSDs. Therefore the security policy language used at the Security Policy Manager Device must be independent of the security protocols of NSDs) policy language (column 4line 65 to column 5 line 3), and

a plurality of computer devices within the distributed security system comprising at least first and second computer devices which process data in accordance

with the security policy of the distributed security system (figure 3A and associated text);

wherein the security policy is configurable to be simultaneously implemented for the plurality of computer devices within the distributed security system, wherein at least a first computer device within the distributed security system operates on an operating platform that supports at least one security protocol that is different than a security protocol supported by a platform of at least a second computer device among the plurality of computer devices (col. 13 line 30 to col. 14 line 45) wherein the first and second computer devices process the data in accordance with security policy of the distributed security system (Fig 2 and column 8 line 49 to 65).

Rothermel teaches distribution and implementation of a security policy in network devices running different security protocols. This would require that the policy be matched with different security protocol (see above). However, Rothermel does explicitly discuss using abstract of the security layer as the way of implementing such feature. Therefore, Rothermel does not teach abstract cryptographic objects such that the security policy is implemented independent of a plurality of underlying cryptographic technologies.

Gen, is directed to a system for solving the problem of providing and interfacing a number of different security mechanisms in a data processing environment (see abstract). In this regard, Gen paragraph [0020] teaches MAL modules, which are abstraction of security mechanisms (also see figure 1 and associated text), that make no distinction between different security mechanism. Hence MAL modules implement security independent of the underlying security mechanisms. Gen also names different cryptographic technologies as security mechanisms in paragraph [0017], where it mentions Kerberos Version 5 and PKI as example security mechanisms that work with its abstraction layer MAL, and particularly mentions that said security mechanisms include different cryptographic technologies (see paragraph [0017]). Therefore, Gen teaches abstract cryptographic objects such that the security policy is implemented independent of a plurality of underlying cryptographic technologies. Note that cryptographic objects were well known in the art at the time of invention. For example, see US 6,470447.

Rothermel and Gen are analogous art, as they are both directed to implementation of security in network nodes running different mechanisms and protocols. At the time of the invention, it would have been obvious by the one skilled in art to use teachings of Gen, particularly the use of abstraction security layers, which are independent of cryptographic protocols, in implementing the system of Rothermel, which implements security protocol independent security

policies. The one skilled in art would be motivated to do so because Gen's teaching provides a way of implementing the details Rothermels system.

Rothermel in view of Gen also teaches wherein the first computer device performs authentication and processes data in accordance with the security policy according to a first cryptographic technique and the second computer device performs authentication and processes data in accordance with the security policy according to a second cryptographic technique, the first cryptographic technique different from the second cryptographic technique (both Rothermel and Gen are directed to performing security actions such as authentication, in network nodes including varying security protocols and mechanisms. Gen paragraph [0017] particularly mentions performing authentication).

6.2. As per claim 2, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:
the security policy identifies the components of the security system (column 5 line 14 to 25).

6.3. As per claim 3, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy identifies the access rights of the security system (column 11 line 18 to 45).

6.4. As per claim 5, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy is configurable (column 7 line 25 to 37).

6.5. As per claim 6, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy language comprises at least some logic based components. As shown in Fig. 3G and column 11 line 45 to 60, the security policy creation template allows the manager to select network security information using radio buttons. Radio buttons corresponds to XOR logic. Therefore, the Examiner asserts that Rothermel policy templates include logic-based components.

6.6. As per claim 7, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy language comprises at least some rule-based components. As shown in Fig. 3D-F and column 11 line 9 to 45, the security policy creation template allows the manager to set the access rules for ping services. Therefore, the Examiner asserts that Rothermel policy templates include ruled-based components.

6.7. As per claim 8, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy language comprises procedural components. As shown in Fig. 3B and column 10 line 24 to 45, a security policy is created based on a procedure of using the policy template and completion of the policy by including network topology attributes. Therefore, the Examiner asserts that Rothermel policy templates include procedural components.

6.8. As per claim 9, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the computer device is configured with computer-executable instructions to:

receive from the first entity a message formatted in a first protocol and transmit to second entity the message formatted in the second protocol that is different from the first protocol (Fig. 6 and column 13 line 30 to 67, and Fig 6 column 13 line 30 to column 14 line 50)

6.9. As per claim 10, Rothermel in view of Gen is directed to the distributed security system of claim 9, wherein:

the computer device is configured with computer-executable instructions to:

receive from the first entity a message transported with a first transport; and

transmit to second entity the message formatted in the second transport that is

different from the first transport (column 16 line 48 to 62, and Fig 6 column 13 line 30 to column 14 line 50)

6.10. As per claim 11 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:
the security policy is implemented in at least one application programming interface (column 13 line 42 to 67).

6.11. As per claim 12 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:
the security language includes programming language constructs (column 13 line 42 to 60).

6.12. As per claim 13 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:
the security policy includes an identify service (Fig. 6 item 640 and column 13 line 45 to 50).

6.13. As per claim 14, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy includes an admission service (Fig. 6 item 630, the firewall will block or admit packets)

6.14. As per claim 15 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy includes a permission service (Fig. 3d and column 11 line 9 to 15).

6.15. As per claim 16 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy includes a revocation service. As indicated in Fig. 3F, the security policy can be configured to allow or disallow a user to access a certain service, such as Ping. Changing the policy to disallow a user to continue accessing a service is analogous to revocation of a right, and therefore works as a revocation service.

6.16. As per claim 17 Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy includes a mapping of entities to rights. As described in Fig. 3B and column 10 line 27 to 65, the policy is created based on security template and attributes of each entity. One of the attributes of each entity is its rights.

Therefore, a policy is created based on the rights of each entity. This discloses the feature.

6.17. As per claim 18, Rothermel in view of Gen is directed to the distributed security system of claim 17, wherein:

the security policy further includes a mapping of entities to capabilities. As described in Fig. 3B and column 10 line 27 to 65, the policy is created based on security template and attributes of each entity. One of the attributes of each entity is its capabilities. Therefore, a policy is created based on the capabilities of each entity. This discloses the feature.

6.18 As per claim 19, Rothermel in view of Gen is directed to the distributed security system of claim 1, wherein:

the security policy is configured to invoke external computer-readable instructions (Fig. 6 and column 13 line 30 to 50).

7. Claims 4, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel in view of Gen as applied to claim 1 above, and further in view of Saulpaugh (U.S. Patent No. 6850979), hereinafter called Sal.

7.1 As per claim 4, Rothermel in view of Gen and Sal is directed to the distributed security system of claim 1, however, it does not include the specific limitation of security policy language comprises the extensible markup language. Saulpaugh teaches a method for creating message gates, useful for controlling the level of security access the client has to the services (column 7 line 36 to 55). Saulpaugh introduces the benefits of using extensible markup language (XML) to create messages gates (column 7 line 19 to 36, column 15 line 62 to column 16 line 35).

Rothermel in view of Gen and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the way that Rothermel distributes security policies between the security manager and the security devices (which in essence, is exchanging a message) using XML comprised message gates as directed by Saulpaugh.

The motivation to do so would have been to improve the security of policy exchange between the security policy manager and network security devices using a standard message exchange language that is interoperable among multiple platforms.

Therefore, it would have been obvious to use XML to create and exchange security policies.

7.2. As per claim 20, Rothermel in view of Gen and Sal is directed to the distributed security system of claim 19, however, it does not include the specific limitation of external computer readable instructions comprise native process code. Saulpaugh teaches a method for creating message gates, useful for invoking programs in computer native language (column 14 line 29 to 42).

Rothermel in view of Gen and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the distributed security system of Rothermel in view of Gen to be capable of invoking programs in computer native language, as described by Saulpaugh.

The motivation to do so would have been to extend the system's range of interoperability to include systems working with machine native language.

7.3. As per claim 21, Rothermel in view of Gen and Sal is directed to the distributed security system of claim 19, however, it does not include the specific limitation of external computer readable instructions comprise Java code. Saulpaugh teaches a method for creating message gates, useful for invoking programs in Java code (column 14 line 29 to 42).

Rothermel in view of Gen and Saulpaugh are analogous art because they are both related to distributed security systems and secure exchange of data between distributed network elements and devices.

At the time of invention, it would have been obvious to a skilled person in the art to improve the distributed security system of Rothermel in view of Gen to be capable of invoking programs in Java code, as described by Saulpaugh.

The motivation to do so would have been to extend the system's range of interoperability to include systems working with Java code.

8. Limitations or claims 33 and 34 are substantially the same as claim 1 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571

272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on (571) 272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Farid Homayounmehr/

Primary Examiner

Art Unit: 2493